

# MetaRule

Impersonation - Carefully check for call failure to avoid unintended privilege escalation

Sean Barnum, Cigital, Inc. [vita<sup>1</sup>]

Copyright © 2007 Cigital, Inc.

2007-03-29

## Part "Original Cigital Coding Rule in XML"

Mime-type: text/xml, size: 10723 bytes

<b>Attack Category</b>	<ul style="list-style-type: none"><li>• Privilege Exploitation</li></ul>																						
<b>Vulnerability Category</b>	<ul style="list-style-type: none"><li>• Privilege escalation problem</li><li>• Process management</li></ul>																						
<b>Software Context</b>	<ul style="list-style-type: none"><li>• Security</li><li>• Process Management</li></ul>																						
<b>Location</b>																							
<b>Description</b>	<p>There are several APIs that are used to temporarily impersonate another security context, often to reduce privilege prior to execution of some capability.</p> <p>If these API calls fail, any further execution of requests could lead to unintended escalation of privilege. It is important to check for failure and not simply continue execution of requests with the assumption that the security context has been changed.</p> <p>If the calling process is running as a highly privileged account, such as LocalSystem, or as a member of an administrative group, the user may be able to perform actions that would otherwise be disallowed.</p>																						
<b>APIs</b>	<table border="1"><thead><tr><th>Function Name</th><th>Comments</th></tr></thead><tbody><tr><td>CAccessToken::Impersonate</td><td>CAccessToken (ATL)</td></tr><tr><td>CAccessToken::ImpersonateLoggedOnUser</td><td>CAccessToken (ATL)</td></tr><tr><td>CoImpersonateClient</td><td>objbase.h</td></tr><tr><td>ImpersonateDdeClientWindow</td><td>ddeml.h</td></tr><tr><td>ImpersonateLoggedOnUser</td><td>winbase.h</td></tr><tr><td>ImpersonateNamedPipeClient</td><td>winbase.h</td></tr><tr><td>ImpersonateSecurityContext</td><td>spi.h</td></tr><tr><td>ImpersonateSelf</td><td>winbase.h</td></tr><tr><td>DdeImpersonateClient</td><td>ddeml.h</td></tr><tr><td>RpcImpersonateClient</td><td>rpc.h</td></tr></tbody></table>	Function Name	Comments	CAccessToken::Impersonate	CAccessToken (ATL)	CAccessToken::ImpersonateLoggedOnUser	CAccessToken (ATL)	CoImpersonateClient	objbase.h	ImpersonateDdeClientWindow	ddeml.h	ImpersonateLoggedOnUser	winbase.h	ImpersonateNamedPipeClient	winbase.h	ImpersonateSecurityContext	spi.h	ImpersonateSelf	winbase.h	DdeImpersonateClient	ddeml.h	RpcImpersonateClient	rpc.h
Function Name	Comments																						
CAccessToken::Impersonate	CAccessToken (ATL)																						
CAccessToken::ImpersonateLoggedOnUser	CAccessToken (ATL)																						
CoImpersonateClient	objbase.h																						
ImpersonateDdeClientWindow	ddeml.h																						
ImpersonateLoggedOnUser	winbase.h																						
ImpersonateNamedPipeClient	winbase.h																						
ImpersonateSecurityContext	spi.h																						
ImpersonateSelf	winbase.h																						
DdeImpersonateClient	ddeml.h																						
RpcImpersonateClient	rpc.h																						

1. [http://buildsecurityin.us-cert.gov/bsi/about\\_us/authors/35-BSI.html](http://buildsecurityin.us-cert.gov/bsi/about_us/authors/35-BSI.html) (Barnum, Sean)

<b>Method of Attack</b>	Elevation of privilege. These calls are frequently used to reduce privilege prior to execution of some capability. However, if any of these calls fail, then the program continues to run at the elevated privilege and is thereby subject to privilege escalation problems.					
<b>Exception Criteria</b>	None noted.					
<b>Solutions</b>	<table border="1"> <thead> <tr> <th data-bbox="807 371 1110 416"><b>Solution Applicability</b></th> <th data-bbox="1123 371 1426 416"><b>Solution Description</b></th> </tr> </thead> <tbody> <tr> <td data-bbox="807 425 1110 676">Generally applicable.</td> <td data-bbox="1123 425 1426 676">Always check the return value of the call, and if it fails do not continue execution of the client request as the security context will remain that of the current process.</td> </tr> </tbody> </table>	<b>Solution Applicability</b>	<b>Solution Description</b>	Generally applicable.	Always check the return value of the call, and if it fails do not continue execution of the client request as the security context will remain that of the current process.	
<b>Solution Applicability</b>	<b>Solution Description</b>					
Generally applicable.	Always check the return value of the call, and if it fails do not continue execution of the client request as the security context will remain that of the current process.					
<b>Signature Details</b>	<p>Standard calls to any of the enumerated APIs, such as:</p> <p>BOOL  ImpersonateSelf(SEcurity_IMPERSONATION_LEVEL ImpersonationLevel);  BOOL DdeImpersonateClient(HCONV hConv);  RPC_STATUS RPC_ENTRY  RpcImpersonateClient(RPC_BINDING_HANDLE BindingHandle);</p>					
<b>Examples of Incorrect Code</b>	<pre>// No check on ret { WDML_CONV* pConv; HCONV hConv; BOOL ret = FALSE;  TRACE("(%p)\n", hConv);  EnterCriticalSection(&amp;WDML_CritSect); pConv = WDML_GetConv(hConv, TRUE); if (pConv) { ret = DdeImpersonateClient(hConv); } LeaveCriticalSection(&amp;WDML_CritSect); return ret; }</pre> <pre>/* No check on call */ /* Obtain the security descriptor. */ if (!GetFileSecurity (path, OWNER_SECURITY_INFORMATION   GROUP_SECURITY_INFORMATION   DACL_SECURITY_INFORMATION,</pre>					

```

pSD, nLength, &nLength))
{
printf ("Unable to obtain
security descriptor.");
return (0);
}
/* Perform security impersonation
of the user and open */
/* the resulting thread token. */
return_bool = ImpersonateSelf
(SecurityImpersonation);
[...]

```

```

// Return code not checked
DWORD dwGuiThreadId = 0;

int UserMessageBox(
RPC_BINDING_HANDLE h,
LPSTR lpszWindowStation,
LPSTR lpszDesktop,
LPSTR lpszText,
LPSTR lpszTitle,
UINT fuStyle)
{
DWORD dwThreadId;
HWINSTA hwinstaSave;
HDESK hdeskSave;
HWINSTA hwinstaUser;
HDESK hdeskUser;
int result;

// Ensure connection to service
window station and desktop, and
// save their handles.

GetDesktopWindow();
hwinstaSave =
GetProcessWindowStation();
dwThreadId =
GetCurrentThreadId();
hdeskSave =
GetThreadDesktop(dwThreadId);

// Impersonate the client and
connect to the User's
// window station and desktop.
RpcImpersonateClient(h);
hwinstaUser =
OpenWindowStation(lpszWindowSt-
ation, FALSE, MAXIMUM_ALLOWED);
if (hwinstaUser == NULL)
{
RpcRevertToSelf();
return 0;
}
}

```

	<pre>SetProcessWindowStation(hwinst- aUser); [...]</pre>
<p><b>Examples of Corrected Code</b></p>	<pre>{ WDML_CONV* pConv; HCONV hConv; BOOL ret = FALSE;  TRACE("(%p)\n", hConv);  EnterCriticalSection(&amp;WDML_CritSect); pConv = WDML_GetConv(hConv, TRUE); if (pConv) { ret = DdeImpersonateClient(hConv); /* Check ret value here and perform algorithm appropriate response */ if (ret != 0) {RevertToSelf(); /*handle error*/ } } LeaveCriticalSection(&amp;WDML_CritSect); return ret; }  [...]</pre> <pre>/* Obtain the security descriptor. */ if (!GetFileSecurity (path, OWNER_SECURITY_INFORMATION   GROUP_SECURITY_INFORMATION   DACL_SECURITY_INFORMATION, pSD, nLength, &amp;nLength)) { printf ("Unable to obtain security descriptor."); return (0); } /* Perform security impersonation of the user and open */ /* the resulting thread token. */ if (!ImpersonateSelf (SecurityImpersonation)) { printf ("Unable to perform security impersonation."); return (0); }  [...]</pre>

	<pre>// Checks return code status = RpcImpersonateClient(Binding); if (status != RPC_S_OK) { #ifdef _DEBUG DisplayError("RpcImpersonateClient", TRUE); #endif return(RPC_S_ACCESS_DENIED); } </pre>				
<b>Source References</b>	<ul style="list-style-type: none"> <li>Howard, Michael &amp; LeBlanc, David C. <i>Writing Secure Code, 2nd ed.</i> Redmond, WA: Microsoft Press, 2002, ISBN: 0735617228.</li> <li><a href="http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnsecure/html/appsec.asp">http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnsecure/html/appsec.asp</a><sup>2</sup></li> <li><a href="http://msdn.microsoft.com/library/default.asp?url=/library/en-us/secauthz/security/impersonateself.asp">http://msdn.microsoft.com/library/default.asp?url=/library/en-us/secauthz/security/impersonateself.asp</a><sup>3</sup></li> <li><a href="http://lists.samba.org/archive/samba-technical/2003-August/031368.html">http://lists.samba.org/archive/samba-technical/2003-August/031368.html</a></li> <li><a href="http://msdn.microsoft.com/library/default.asp?url=/library/en-us/winui/winui/windowsuserinterface/sec_winui.asp">http://msdn.microsoft.com/library/default.asp?url=/library/en-us/winui/winui/windowsuserinterface/sec_winui.asp</a><sup>5</sup></li> <li><a href="http://msdn.microsoft.com/library/default.asp?url=/library/en-us/winui/winui/windowsuserinterface/dataexchange/dynamicdataexchangemanagementlibrary/dynamicdataexchangemanagementreference/dynamicdataexchangemanagementfunctions/ddeimpersonateclient.asp">http://msdn.microsoft.com/library/default.asp?url=/library/en-us/winui/winui/windowsuserinterface/dataexchange/dynamicdataexchangemanagementlibrary/dynamicdataexchangemanagementreference/dynamicdataexchangemanagementfunctions/ddeimpersonateclient.asp</a><sup>6</sup></li> <li><a href="http://msdn.microsoft.com/library/default.asp?url=/library/en-us/rpc/rpc/rpcimpersonateclient.asp">http://msdn.microsoft.com/library/default.asp?url=/library/en-us/rpc/rpc/rpcimpersonateclient.asp</a><sup>7</sup></li> <li><a href="http://groups-beta.google.com/group/microsoft.public.win32.programmer.networks/browse_thread/thread/52a5e9311cff8595/93fd5b5e62828b0d?q=rpcimpersonateclient+check+return&amp;rnum=2&amp;hl=en#93fd5b5e62828b0d">http://groups-beta.google.com/group/microsoft.public.win32.programmer.networks/browse_thread/thread/52a5e9311cff8595/93fd5b5e62828b0d?q=rpcimpersonateclient+check+return&amp;rnum=2&amp;hl=en#93fd5b5e62828b0d</a><sup>8</sup></li> </ul>				
<b>Recommended Resource</b>					
<b>Discriminant Set</b>	<table border="1"> <tr> <td data-bbox="798 1653 1117 1713"> <b>Operating System</b> </td> <td data-bbox="1117 1653 1442 1713"> <ul style="list-style-type: none"> <li>Windows</li> </ul> </td> </tr> <tr> <td data-bbox="798 1713 1117 1809"> <b>Languages</b> </td> <td data-bbox="1117 1713 1442 1809"> <ul style="list-style-type: none"> <li>C</li> <li>C++</li> </ul> </td> </tr> </table>	<b>Operating System</b>	<ul style="list-style-type: none"> <li>Windows</li> </ul>	<b>Languages</b>	<ul style="list-style-type: none"> <li>C</li> <li>C++</li> </ul>
<b>Operating System</b>	<ul style="list-style-type: none"> <li>Windows</li> </ul>				
<b>Languages</b>	<ul style="list-style-type: none"> <li>C</li> <li>C++</li> </ul>				

## Cigital, Inc. Copyright

Copyright © Cigital, Inc. 2005-2007. Cigital retains copyrights to this material.

Permission to reproduce this document and to prepare derivative works from this document for internal use is granted, provided the copyright and “No Warranty” statements are included with all reproductions and derivative works.

For information regarding external or commercial use of copyrighted materials owned by Cigital, including information about “Fair Use,” contact Cigital at [copyright@cigital.com](mailto:copyright@cigital.com)<sup>1</sup>.

The Build Security In (BSI) portal is sponsored by the U.S. Department of Homeland Security (DHS), National Cyber Security Division. The Software Engineering Institute (SEI) develops and operates BSI. DHS funding supports the publishing of all site content.

---

1. <mailto:copyright@cigital.com>